Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

Analytic Functions Suitable to Represent Substitutions.

BY LEONARD E. DICKSON.

1. To Hermite* is due the theorem:

In order that the reduced function $\phi(x)$ shall represent a substitution on p letters, p being prime, it is necessary and sufficient that, on raising $\phi(x)$ to the powers $2, 3, \ldots p-2$, and reducing the results by the congruence $x^{p-1} \equiv 1$ (mod. p), the terms independent of x be congruent to zero.

By the *reduced form* of the function $\theta(x)$ is meant the function

$$\phi(x) = \alpha\theta(x+\beta)+\gamma,$$

when α, β, γ are so chosen that the coefficient of the highest power of x in $\phi(x)$ is unity, that of the next highest power zero, and the independent term zero.

2. Theorem: The reduced function $x^k + ax^{k-2} + bx^{k-3} + \ldots + lx$, where $k > 1$, is not suitable to represent a substitution on p letters, if p be a prime number of the form $nk+1$.

For on raising it to the power $\frac{p-1}{k} = n$ and reducing by $x^{p-1} \equiv 1$ (mod. p), the independent term is 1.

3. The reduced function x is suitable for any prime p; but x^2 is suitable for no odd prime p.

4. Reduced form $x^3 + ax$. $p = 3n+2$.

$$(x^3+ax)^{n+1} = x^{3n+3} + (n+1)ax^{3n+1} + \text{lower powers of } x.$$
$$\equiv x^2 + (n+1)a + \text{powers of } x \pmod{3n+2}.$$

$\therefore a \equiv 0$. But the exponent of x in $(x^3)^k$, for $k < 3n+1$, is not divisible by $3n+1$. Thus x^3 is the only suitable reduced form of the third degree.

---

* Comptes Rendus, vol. 57, p. 750.

5. Reduced form $x^4 + ax^2 + bx$. $p = 4n + 3$.

$$(x^4 + ax^2 + bx)^{n+1} = x^{4n+4} + (n+1)\,ax^{4n+2} + \text{lower powers of } x.$$

$$\therefore\ a \equiv 0 \pmod{4n+3}.$$

$$(x^4 + bx)^{n+2} = x^{4n+8} + (n+2)\,bx^{4n+5} + \frac{(n+2)(n+1)}{1.2}\,b^2x^{4n+2} + \ldots .$$

(1). If $p > 7$, this is $\equiv x^6 + (n+2)\,bx^3 + \tfrac{1}{2}(n+2)(n+1)\,b^2 + \text{terms in } x \pmod{4n+3}$. $\therefore\ b \equiv 0$. But $(x^4)^{2n+1} = x^{8n+4} \equiv 1 \pmod{4n+3}$. Hence, for $p > 7$, no form of the fourth degree can represent a substitution on a prime number of letters.

(2). If $p = 7$, $(x^4 + bx)^3 \equiv (1 + 3b^2) + 3bx^3 + b^3x^3 \pmod{7}$. $\therefore\ 3b^2 + 1 \equiv 0$. $\therefore\ b \equiv \pm 3 \pmod{7}$. Evidently the fourth and fifth powers of $x(x^3 \pm 3)$ contain no term whose exponent is divisible by 6, and hence no constant term when reduced by $x^6 \equiv 1 \pmod{7}$. Hence $x^4 \pm 3x$ represents substitutions on 7 letters.

6. Reduced form $x^5 + ax^3 + bx^2 + cx$.

Let $p = 5n + 2$.

$$(x^5 + ax^3 + bx^2 + cx)^{n+1} \text{ requires } (n+1)\,c + \frac{n(n+1)}{1.2}\,a^2 \equiv 0 \pmod{5n+2}.$$

$$\therefore\ 2c + na^2 \equiv 0, \text{ or } c \equiv (2n+1)\,a^2. \quad \therefore\ 5c \equiv a^2 \pmod{5n+2}.$$

The power $(n+2)$ requires that $6abc + b^3 + (n-1)\,a^3b \equiv 0$, when $p > 7$. Applying $2c \equiv -na^2$, this becomes $b\,\{b^2 - (2n+1)\,a^3\} \equiv 0$. The power $(n+3)$ requires, for $p > 7$,

$$\frac{(n+3)(n+2)(n+1)\,n}{1.2.3.4}\left\{4ac^3 + 6b^2c^2 + \frac{n-1}{5}\,(10a^3c^2 + 30a^2b^2c + 5ab^4) + \frac{(n-1)(n-2)}{5.6}\,(6a^5c + 15a^4b^2) + \frac{(n-1)(n-2)(n-3)}{5.6.7}\,a^7\right\} \equiv 0.$$

Multiplying the quantity in brackets by $5^3.6.7$ and reducing by $5c \equiv a^2$, $5(n-1) \equiv -7$, $5(n-2) \equiv -12$, etc., this gives $b^2(6a^4 - 35ab^2) \equiv 0$.

Suppose $b \not\equiv 0$. $\therefore\ 6a^4 - 35ab^2 \equiv 0$. Also $b^2 - (2n+1)\,a^3 \equiv 0$.

$$\therefore\ 6a^4 - 35a^4(2n+1) \equiv 0 \text{ or } -a^4 \equiv 0 \pmod{5n+2}. \quad \therefore\ a \equiv 0 \text{ and } b \equiv 0.$$

Thus the conditions required by the above three powers of our form are satisfied, for $p > 7$, only when $5c \equiv a^2$, $b \equiv 0$, giving the form $5x^5 + 5ax^3 + a^2x$.

7. The case $p = 7$ is discussed by Hermite.

The square, cube and fourth power give $2c + a^2 \equiv 0$; $b(3 + 6ac + b^2) \equiv 0$; $ab^2 + 4b^2c^2 + 2(2a + c^2)(1 + 2ac + b^2) \equiv 0$. If we take $b \equiv 0$ and apply $c \equiv 3a^2$ to the third congruence, it reduces to the identity $2(a - a^7) \equiv 0 \pmod{7}$. If we take $b \not\equiv 0$ and apply $c \equiv 3a^2$ to the second and third congruences, they reduce to $b^2 - 3a^3 + 3 \equiv 0$; $a + a^4 \equiv 0$. Whence follow two solutions $a \equiv 0$, $b \equiv \pm 2$, and $a^3 \equiv -1$, $b \equiv \pm 1 \pmod{7}$. Thus $p = 7$ leads to the forms $x^5 + ax^3 + 3a^2x$ or $5x^5 + 5ax^3 + a^2x$, a being indeterminate; $x^5 \pm 2x^2$; $x^5 + ax^3 \pm x^2 + 3a^2x$, a being a quadratic non-residue of 7.

8. Let $p = 5n + 3$, n being even.

$(x^5 + ax^3 + bx^2 + cx)^{n+1}$ gives $b \equiv 0 \pmod{5n + 3}$.

$$(x^5 + ax^3 + cx)^{n+2} \text{ gives } \frac{(n+2)(n+1)}{1.2}c^2 + \frac{(n+2)(n+1)n}{1.2.3}.3a^2c$$
$$+ \frac{(n+2)(n+1)n(n-1)}{1.2.3.4}a^4 \equiv 0.$$

$\therefore\ 12c^2 + 12na^2c + n(n-1)a^4 \equiv 0.$

$36c^2 + 36na^2c + 9a^4n^2 \equiv 9a^4n^2 - 3n(n-1)a^4 \equiv a^4n^2 \pmod{5n + 3}.$

$\therefore\ 6c + 3a^2n \equiv \pm a^2n. \quad \therefore\ 3c \equiv -a^2n$ or $-2a^2n.$

Hence $c \equiv (3n + 2)a^2$ or $(n + 1)a^2$.

The odd powers of $x^5 + ax^3 + cx$ give no terms with even exponent, and hence no constant term upon reduction by $x^{5n+2} \equiv 1 \pmod{5n + 3}$.

For $p > 13$, $(x^5 + ax^3 + cx)^{n+4}$ gives

$$c_5^{n+4}.5ac^4 + c_6^{n+4}.20a^3c^3 + c_7^{n+4}.21a^5c^2 + c_8^{n+4}.8a^7c + c_9^{n+4}.a^9 \equiv 0,$$

where c_r^m denotes the binomial coefficient $\dfrac{m(m-1)\ldots\ldots(m-r+1)}{1.2\ldots\ldots r}$. Dividing out the factor $n(n + 1)(n + 2)(n + 3)(n + 4)$ and multiplying by $5^4.7\,!$, we find:

$$210a(5c)^4 + 140a^3.5(n-1)(5c)^3 + 21a^5.5^2(n-1)(n-2)(5c)^2$$
$$+ 5^3(n-1)(n-2)(n-3)a^7(5c) + \frac{5^4(n-1)(n-2)(n-3)(n-4)}{8.9}a^9 \equiv 0.$$

Since $5(n-1) \equiv -8$, $5(n-2) \equiv -13$, etc., this becomes:

$$210a(5c)^4 - 8.140a^3(5c)^3 + 8.13.21a^5(5c)^2 - 8.13.18a^7(5c) + 2.13.23a^9 \equiv 0.$$

(1). $c \equiv (3n + 2)a^2$. $\quad \therefore\ 5c \equiv a^2$.

$\therefore\ a^9(210 - 8.140 + 8.13.21 - 8.13.18 + 2.13.23) \equiv 0$. The coefficient of a^9 is seen to be zero. The condition is therefore satisfied for $5c \equiv a^2$, a being arbitrary.

(2). $c \equiv a^2(n+1)$. $\therefore$ $5c \equiv 2a^2$.

$\therefore$ $a^9\,(210.2^4 - 8.140.2^3 + 8.13.21.2^2 - 8.13.18.2 + 2.13.23) \equiv 0$.

$\therefore$ $-10a^9 \equiv 0$ (mod. $5n+3$). $\therefore$ $a \equiv 0$ and $c \equiv 0$.

Thus for $p > 13$ the reduced quintic form must be equivalent to the form $5x^5 + 5ax^3 + a^2x$.

9. For $p = 13$, $c \equiv -5a^2$ or $3a^2$.

$(x^5 + ax^3 + cx)^6$ gives $10a\,(1 + c^3)(3c + 2a^2) \equiv 0$. For $c \equiv -5a^2$ this reduces to an identity. For $c \equiv 3a^2$ it becomes $6a^3\,(1 + a^6) \equiv 0$. $\therefore$ a is either $\equiv 0$ or a quadratic non-residue of 13.

$(x^5 + ax^3 + cx)^8$ gives $(5c^4 + a^2c^3 + 4a^4c^2 + 4a^6c + a^8) + (c^6 + 1)(8c + 2a^2) \equiv 0$.

The first expression reduces to an identity for $c \equiv -5a^2$ or $3a^2$. $c^6 + 1 \equiv 0$ (mod. 13) if $c \equiv -5a^2$; $8c + 2a^2 \equiv 0$ (mod. 13) if $c \equiv 3a^2$. $(x^5 + ax^3 + cx)^{10}$ gives $10a\,(c^9 + 1) + a\,(c^3 + 1)(8c^3 - 2a^2c^2 - a^4c + 3a^6) \equiv 0$. For $c \equiv 3a^2$ this becomes $10a\,(a^{18} + 1) + 3a^7\,(a^6 + 1) \equiv 3a\,(a^6 + 1)(a^6 - 1) \equiv 0$ (mod. 13). For $c \equiv -5a^2$ it becomes the identity $10a\,(1 - 5a^{18}) + 11a^7\,(1 + 5a^6) \equiv 0$ (mod. 13).

Thus all conditions are satisfied by the forms: $x^5 + ax^3 + 3a^2x$, where a is a quadratic non-residue of 13, and $x^5 + ax^3 - 5a^2x$, where a is arbitrary. The last form is equivalent to $5x^5 + 5ax^3 + a^2x$.

10. Let $p = 5n + 4$.

$(x^5 + ax^3 + bx^2 + cx)^{n+1}$ gives $a \equiv 0$. $(x^5 + bx^2 + cx)^{n+2}$ gives $bc \equiv 0$. $(x^5 + bx^2 + cx)^{n+3}$ gives $4c^3 + nb^4 \equiv 0$. Hence $b \equiv 0$, $c \equiv 0$, and x^5 is the only suitable function.

11. We have seen that every function of the fifth degree suitable to represent a substitution must be reducible to the form $5x^5 + 5ax^3 + a^2x$ when $p > 13$. Inversely, for $p = 5n + 2$ or $5n + 3$, the function $5x^5 + 5ax^3 + a^2x$ is always suitable to represent a substitution on a prime number p of letters, i. e. will run through a complete system of residues modulo p simultaneously with x.

For, if not, we must have for two values of x, incongruent modulo p, say x and y, the following congruence:

$$5x^5 + 5ax^3 + a^2x \equiv 5y^5 + 5ay^3 + a^2y \text{ (mod. } p).$$

$$\therefore\ (x - y)\,\{5\,(x^4 + x^3y + x^2y^2 + xy^3 + y^4) + 5a\,(x^2 + xy + y^2) + a^2\} \equiv 0.$$

$$\therefore\ 5\,\{x^4 + y^4 + (xy + a)(x^2 + xy + y^2)\} + a^2 \equiv 0.$$

Put $x = u + v$, $y = u - v$.

$$\therefore\ 5\{2u^4 + 12u^2v^2 + 2v^4 + (u^2 - v^2 + a)(3u^2 + v^2)\} + a^2 \equiv 0.$$

or $$5\{5u^4 + 10u^2v^2 + v^4 + 3au^2 + av^2\} + a^2 \equiv 0.$$

Put $u^2 = \alpha$, $v^2 = \beta$.

$$\therefore\ 25\alpha^2 + 50\alpha\beta + 5\beta^2 + 15a\alpha + 5a\beta + a^2 \equiv 0.$$

Transform (to center of conic) by writing $\alpha \equiv X - \frac{a}{20}$, $\beta \equiv Y - \frac{a}{4}$, or by the integral expressions:

$$20X \equiv 20\alpha + a,\quad 4Y \equiv 4\beta + a \pmod{p}.$$

The constant term is seen to vanish, giving

$$25X^2 + 50XY + 5Y^2 \equiv 0,$$

or $$(5X + 5Y)^2 \equiv 20Y^2 = 5(2Y)^2 \pmod{p}.$$

Hence 5 must be a quadratic residue of p. But, by Gauss, D. A., Art. 121, $+5$ is a quadratic residue of *no* odd prime number of the form $5n + 2$ or $5n + 3$.

12. Of the forms $\phi(x) = 5x^5 + 5ax^3 + a^2x$, given by the values $1, 2, \ldots (p-1)$ of a, to find those independent ones to which all the others can be *reduced.* Suppose the form given by a' can be reduced to that given by a. Then $5x^5 + 5a'x^3 + a'^2x$ must be identical with $\alpha\phi(\beta x) = 5\alpha\beta^5x^5 + 5\alpha\beta^3ax^3 + \alpha\beta a^2x$, where α and β must thus satisfy the conditions $\alpha\beta^5 \equiv 1$, $\alpha\beta^3a \equiv a'$, $\alpha\beta a^2 \equiv a'^2$ (mod. p). These three conditions reduce to two independent ones: $\alpha\beta^5 \equiv 1$, $a \equiv a'\beta^2$ (mod. p). Hence the necessary and sufficient condition that the forms corresponding to a and a' shall be reducible one to the other is that a and a' be both quadratic residues or both non-residues of p. Hence there are just two such independent forms.

13. Of interest is the case $a' = p - a$. Then $\beta^2 \equiv -1$ (mod. p). The reduction can thus be effected if p be of the form $4n + 1$.

Let $x = \beta X$. Then

$$5x^5 + 5a'x^3 + a'^2x \equiv 5x^5 - 5ax^3 + a^2x \equiv \beta X(5X^4 + 5aX^2 + a^2) \pmod{p}.$$

$$\therefore\ \beta(5X^5 + 5aX^3 + a^2X) \equiv 5(\beta X)^5 + 5a'(\beta X)^3 + a'^2(\beta X).$$

Hence if the substitution corresponding to the form given by a is $\begin{pmatrix} c, & d, & e, & \ldots & h \\ C, & D, & E, & \ldots & H \end{pmatrix}$, that corresponding to the form given by a' will be $\begin{pmatrix} \beta c, & \beta d, & \beta e, & \ldots & \beta h \\ \beta C, & \beta D, & \beta E, & \ldots & \beta H \end{pmatrix}$.

Example: $p = 17$. $\therefore\ \beta \equiv 4$. Table for $x^5 + ax^3 + 7a^2x$:

$$\left\{\begin{array}{ll} a = 8, & (4, 13)(5, 7, 9, 12, 10, 8)(1, 15, 11, 14, 16, 2, 6, 3). \\ a' = 9, & (16, 1)(3, 11, 2, 14, 6, 15)(4, 9, 10, 5, 13, 8, 7, 12). \end{array}\right.$$

$$\left\{\begin{array}{ll} a = 7, & (1, 11, 10, 15, 8, 13, 12, 14)(2, 9, 4, 5, 3, 16, 6, 7). \\ a' = 10, & (4, 10, 6, 9, 15, 1, 14, 5)(8, 2, 16, 3, 12, 13, 7, 11). \end{array}\right.$$

$$\left\{\begin{array}{ll} a = 5, & (7, 10)(1, 11, 5)(6, 12, 16)(2, 14, 15, 3),\ 4, 8, 9, 13 \text{ being unchanged.} \\ a' = 12, & (11, 6)(4, 10, 3)(7, 14, 13)(8, 5, 9, 12),\ 16, 15, 2, 1 \text{ being unchanged.} \end{array}\right.$$

14. For $p = 13$, the forms (additional to the forms $5x^5 + 5ax^3 + a^2x$ existing also in the general case) $x^5 + ax^3 + 3a^2x$, where a is a non-residue of 13, all *reduce* to a single one.

For $p = 7$, the additional forms $x^5 \pm 2x^2$ and $x^5 + ax^3 \pm x + 3a^2x$, a being a non-residue of 7, reduce to $x^5 + 2x^2$ and $x^5 + 3x^3 + x^2 - x$ respectively.

15. Reduced form $x^6 + ax^4 + bx^3 + cx^2 + dx$. $p = 6n + 5$. The power $n + 1$ gives $a \equiv 0$. $(x^6 + bx^3 + cx^2 + dx)^{n+2}$ gives $c^2 + 2bd \equiv 0$. The power $n + 3$ gives, for $p > 11$,

$$\frac{(n+3)(n+2)(n+1)}{1.2.3}\left\{3cd^2 + \frac{n}{4}(4b^3d + 6b^2c^2)\right\} \equiv 0.$$

The power $(n + 4)$ gives, for $p > 17$,

$$\frac{(n+4)(n+3)(n+2)(n+1)}{1.2.3.4}\left\{d^4 + \frac{n}{5}(30b^2cd^2 + 20bc^3d + c^5) + \frac{n(n-1)}{5.6}(6b^5d + 15b^4c^2)\right\} \equiv 0.$$

$$\therefore \begin{cases} (1)\ c^2 + 2bd \equiv 0, \\ (2)\ 6cd^2 + 2nb^3d + 3nb^2c^2 \equiv 0, \\ (3)\ 10d^4 + 60nb^2cd^2 + 40nbc^3d + 2nc^5 + n(n-1)(2b^5d + 5b^4c^2) \equiv 0. \end{cases}$$

Substituting $c^2 \equiv -2bd$ in (2) and (3), they become

$$6cd^2 - 4nb^3d \equiv 0.$$

$$10d^4 - 12nb^2cd^2 - 8n(n-1)b^5d \equiv 0. \tag{4}$$

From the last two,

$$10d^4 - 8n(2n-1)b^5d \equiv 0. \tag{5}$$

Multiplying (1) by nb^2 and subtracting from (2),

$$6cd^2 + 2nb^2c^2 \equiv 0.$$

Suppose $c \not\equiv 0$. $\therefore\ 3d^2 + nb^2c \equiv 0$.

Hence, substituting in (4),

$$46d^4 - 8n(n-1)b^5d \equiv 0.$$

Combining with (5),

$$d^4\{46(2n-1) - 10(n-1)\} \equiv 0.$$

$$\therefore\ 313d^4 \equiv 0 \ (\text{mod. } 6n+5). \quad \therefore\ d \equiv 0.$$

Hence c must be $\equiv 0$. $\therefore\ bd \equiv 0$. $\therefore$ by (5), $d \equiv 0$. But $(x^6 + bx^3)^{3n+2}$ gives x^{18n+12} and no other term with exponent divisible by $6n+4$. Hence no function of the sixth degree can represent a substitution on a prime number of letters > 17.

16. $p = 11$.

As before, $$a \equiv 0\,;\ c^2 + 2bd \equiv 0. \qquad (1)$$

The fourth and fifth powers now give:

$$4c + 4b^3d + 6b^2c^2 + 12d^2c \equiv 0, \qquad (2)$$

$$1 + 10d^2 + 30b^2c + 5d^4 + 30b^2cd^2 + 20bc^3d + c^5 \equiv 0. \qquad (3)$$

Multiplying (1) by $2b^2$ and subtracting from (2),

$$c(1 + b^2c + 3d^2) \equiv 0.$$

(1). Suppose $c \equiv 0$. (3) becomes $1 + 10d^2 + 5d^4 \equiv 0$ (mod. 11).

$\therefore\ (d^4 + 2d^2 - 2) \equiv 0$, or $(d^2 - 4)(d^2 - 5) \equiv 0$. $\therefore\ d \equiv \pm 2$ or ± 4.

Now $bd \equiv 0$. Hence, since $d \not\equiv 0$, $b \equiv 0$.

Evidently $x(x^5 + d)$, when raised to the power 6, 7, 8 or 9, will contain no exponent divisible by 10. Hence the forms $x^6 \pm 2x$ and $x^6 \pm 4x$ satisfy all conditions.

(2). Suppose $c \not\equiv 0$. $\therefore\ 3d^2 + b^2c + 1 \equiv 0$.

Reducing (3) by $c^2 \equiv -2bd$, it becomes

$$1 + 10d^2 + 5d^4 - 3b^2c + 5b^2cd^2 \equiv 0. \qquad (4)$$

Applying $b^2c \equiv -1 - 3d^2$, (4) gives $d^4 + 3d^2 + 4 \equiv 0$.

$$\therefore\ (d^2 - 3)(d^2 - 5) \equiv 0 \ (\text{mod. } 11). \quad \therefore\ d \equiv \pm 4 \text{ or } \pm 5.$$

For $\quad d \equiv \pm 5,\ b^2c \equiv 1,\ c^2 \equiv \pm\ b. \ \therefore\ c^5 \equiv +1.$

For $\quad d \equiv \pm 4,\ b^2c \equiv 6,\ c^2 \equiv \pm 3b. \ \therefore\ c^5 \equiv -1.$

Hence the forms satisfying conditions (1), (2), (3) are:

$$\begin{cases} x^6 \pm\ c_1^{\frac{3}{2}}x^3 + c_1x^2 \pm 5x, & \text{where } c_1 \text{ is a quadratic residue of } 11. \\ x^6 \pm 4c_2^{\frac{3}{2}}x^3 + c_2x^2 \pm 4x, & \text{where } c_2 \text{ is a quadratic non-residue of } 11. \end{cases}$$

We can verify that the conditions obtained by raising $(x^6 + bx^3 + cx^2 + dx)$ to the powers 6, 7, 8 and 9 are satisfied. The 6th power gives

$$b^2 + 6b^2d^2 + 12bc^2d + c^4 + 2b^4c + b^2d^4 + 4bc^2d^3 + c^4d^2 \equiv 0.$$

Applying $c^2 \equiv -2bd$, this becomes

$$b^2 - 3b^2d^2 + 2b^4c - 3b^2d^4 \equiv 0.$$

Applying $b^2c \equiv -1 - 3d^2$ to the latter,

$$b^2(1 - 2d^2 + 3d^4) \equiv 0,$$

equivalent to $d^4 + 3d^2 + 4 \equiv 0$.

The 7th power gives

$$30bcd + 5c^3 + 5b^4 + 60bcd^3 + 30c^3d^2 + 15b^4d^2 + 60b^3c^2d$$
$$+ 15b^2c^4 + b^6c + 6bcd^5 + 5c^3d^4 \equiv 0.$$

Applying $c^2 \equiv -2bd$, this reduces to $5b^4 - 2bcd - b^4d^2 + b^6c - 4bcd^5 \equiv 0$. Reducing by $3d^2 \equiv -1 - b^2c$, this gives $b^5d - 2b^2c - 3 \equiv 0$, a form derived from (4) by substituting $d^4 \equiv -3d^2 - 4$ and afterwards $d^2 \equiv -4 - 4b^2c$. Hence the condition is not independent of (1), (2), (3). Similarly for the 8th and 9th powers.

17. $p = 17$.

As in the general case,

$$a \equiv 0;\ c^2 + 2bd \equiv 0, \tag{1}$$
$$3cd^2 + 2b^3d + 3b^2c^2 \equiv 0. \tag{2}$$

But the third condition now contains a term in c, thus:

$$6c + 15d^4 + 180b^2cd^2 + 120bc^3d + 6c^5 + 6b^5d + 15b^4c^2 \equiv 0. \tag{3}$$
$$\therefore\ 3cd^2 - 4b^3d \equiv 0;\ 2c + 5d^4 - 12b^2cd^2 - 8b^5d \equiv 0.$$

From the last two,

$$2c + 5d^4 - b^2cd^2 \equiv 0. \tag{4}$$

As in the general case, if $c \not\equiv 0$, $3d^2 + 2b^2c \equiv 0$ or $d^2 \equiv 5b^2c$.

Substituting in (4), $2c + b^4c^2 \equiv 0$. $\therefore c \equiv b^5d$. Thus $3cd^2 \equiv 4b^3d$ gives $3b^2d^2 \equiv 4$. $\therefore c^4 \equiv -6$ (mod. 17), which is impossible, since it requires $c^{16} \equiv 4$ (mod. 17). Hence $c \equiv 0$ and, as in the general case, the form is rejected.

18. The five pairs of forms $\phi(x) = x^6 \pm c^2x^3 + cx^2 \pm 5x$, where c is a quadratic residue of 11, all reduce to a single form. For the conditions that $\alpha\phi(\beta x) = \alpha\beta^6x^6 \pm \alpha\beta^3c^2x^3 + \alpha\beta^2cx^2 \pm 5\alpha\beta x$ shall be identical with $x^6 \pm c'^2x^3 + c'x^2 \pm 5x$ are

$$\alpha\beta^6 \equiv 1,\quad \alpha\beta^3c^2 \equiv \pm c'^2,\quad \alpha\beta^2c \equiv c',\quad \alpha\beta \equiv \pm 1,$$

which are equivalent to the three:

$$\alpha\beta \equiv \pm 1, \quad \beta^5 \equiv \pm 1, \quad \beta c \equiv \pm c'.$$

Likewise the five pairs of forms $x^6 \pm 4c^2x^3 + cx^2 \pm 4x$, where c is a quadratic non-residue of 11, all reduce to a single form.

19. *Summary.*—Let $\phi(x)$ be an integral function of degree $\leqq 6$ having integral coefficients. Then if $\begin{pmatrix} x \\ \phi(x) \end{pmatrix}$ represents a substitution on a prime number p of letters, the substitution

$$\begin{pmatrix} x \\ ax+b \end{pmatrix}\begin{pmatrix} x \\ \phi(x) \end{pmatrix}\begin{pmatrix} x \\ cx+d \end{pmatrix}$$

may be reduced by properly choosing a, b, c, d and by using if possible $x^p = x \pmod{p}$ to one of the following forms:

Reduced function:	Suitable for:
x	$p = \text{any}$,
x^3	$p = 3n + 2$,
$x^4 + 3x$	$p = 7$,
$5x^5 + 5ax^3 + a^2x$, ($a = 1$ or some one non-residue of p),	
$x^5 + 2x^2$	$p = 7$,
$x^5 + 3x^3 + x^2 - x$	
$x^5 + 2x^3 - x$	$p = 13$,
x^5	$p = 5n + 4$,
$x^6 + 2x$	$p = 11$.
$x^6 + 4x$	
$x^6 + x^3 + x^2 + 5x$	
$x^6 + 5x^3 + 2x^2 + 4x$	

UNIVERSITY OF CHICAGO, *March* 27, 1895.

NOTE OF MARCH, 1896.—Generalizations of these results will appear in a dissertation to be published soon at the University Press.